UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/789,805 | 02/27/2004 | Michael D. Smith | 418268001US | 5629 |

45979 7590 04/03/2009

PERKINS COIE LLP/MSFT
P. O. BOX 1247
SEATTLE, WA 98111-1247

| EXAMINER | |
|---|---|
| STRODER, CARRIE A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 3689 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/03/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/789,805 | SMITH ET AL. | |
| | Examiner | Art Unit | |
| | CARRIE A. STRODER | 3689 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *20 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,5,6 and 9-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5,6 and 9-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20 January 2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**DETAILED ACTION**

1. This is in response to the applicant's communication filed on 20 January 2009, wherein:

Claims 1-2, 5-6, and 9-30 are currently pending.

Claims 3-4 and 7-8 are cancelled.

Claims 1, 10, 17, 23, and 25 are currently amended..

***Information Disclosure Statement***

1. The information disclosure statement (IDS) submitted on 20 January 2009 was filed after the mailing date of the First Office Action on 17 September 2008. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

***Response to Arguments***

2. Applicant's arguments with respect to claims 1, 10, 17, and 23 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the

invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

***Claim Rejections - 35 USC § 103***

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. **Claims 1, 5-6, 10-11, 13-15, 17-24, 26-29 are rejected** under 35 U.S.C. 102(e) as being anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Liang et al. (US 20040205419).

**Referring to claim 1:**

Liang teaches

when installing an application,

establishing a limit on services of a service provider that the application is authorized to use based on published requirements of the application (paragraphs 25-30 and 54; "…the rules engine…can be generated by the server" and "each sensor stores rules for determining abnormality"; where "generated" is interpreted as "published" and "rules for determining abnormality" is interpreted as establishing a limit);

determining by the processor whether the application is authorized to request services of the service provider by asking

the service provider if the application is authorized to use the service provider, wherein the service provider determines that the application is not authorized based on notifications received from other consumer systems indicating that the application is misbehaving (paragraphs 28-30; where it is implied that the anti-virus system will prevent the installation of applications which have been detected to include a virus and the service being provided is the use of the processor or network resources by the application);

when it is determined that the application is authorized to request services of the service provider, installing the application (paragraphs 28-30; where it is implied that when the anti-virus system does not detect a virus, the application will be installed); and

when it is determined that the application is not authorized to request services of the service provider, not installing the application (paragraphs 28-30; where it is implied that when the anti-virus system does detect a virus, the application will not be installed); and

under control of a runtime environment after the application has been installed, providing the application with access to the established limit (paragraphs 28-30; where it is implied that the applications can run up to the limit

established by the "rules for determining abnormality" without interference by the virus detection system);

when the application requests a service of the service provider,

determining by the processor whether the request would exceed the established limit that is based on published requirements of the application (paragraph 30; "process will process the raw data from different sensor issue high-risk alerts if the data reach or exceed certain thresholds");

when it is determined that the request would not exceed the established limit, requesting the service provider to provide the service (paragraph 30; where it is implied that as long as the threshold is not reached, the application will be allowed to run, where "service provider" is interpreted as the processor or network resources running the application); and

when it is determined that the request would exceed the established limit,

notifying the service provider that the application is misbehaving (paragraph 30; "issue high risk alerts"); and

prohibiting execution of the application on the consumer system (paragraphs 25-30 and 54-56; "a segment in the network system including the abnormal device nodes can be partially isolated").

**Referring to claim 10:**

Liang teaches

providing an indication of misbehavior for the application when the application requests services of the service provider (paragraph 25; "rules provider that serves to determine whether the abnormal events are potentially computer viruses"); and

under control a runtime environment,

when the application requests a service of the service provider,

determining by the processor whether the application is behaving in accordance with the indication of the misbehavior (paragraph 30; "continuously monitor system activities" and "each sensor stores rules for determining abnormality");

when it is determined that the application is not behaving in accordance with the indication of misbehavior, requesting the service provider to provide the service (paragraph 30; where it is implied that as long as the threshold is not reached, the application will be allowed to run, where "service provider" is interpreted as the processor or network resources running the application); and

when it is determined that the application is behaving in accordance with the indication of misbehavior,

notifying the service provider that the application is misbehaving so that the service provider can determine with the application is misbehaving and revoke authorization of the application to use the service provider (paragraph 30; "issue high risk alerts"); and

prohibiting execution of the application (paragraphs 25-30 and 54-56; "a segment in the network system including the abnormal device nodes can be partially isolated").

**Referring to claim 23:**

Liang teaches

a component that installs the application on the service consumer when a service provider indicates that the application has not been misbehaving an indicated by notification received by other service consumers and establishes an indication of misbehavior for the application when the application requests services of the service provider (paragraphs 28-30; where it is implied that the anti-virus system will allow the installation of applications which have not been detected to include a virus and the service provider is processor or network resources used by the application); and

a runtime environment that requests the service provider to provide a service when the application requests a service of the service provider and when the application does not behave in

accordance with the established indication of misbehavior for the application, and that notifies the service provider that the application is misbehaving when the application behaves in accordance with the established indication of misbehavior for the application (paragraph 30; where "issue high risk alerts" is interpreted as "notifies").

**Referring to claims 5, 14 and 28:**

Claims 5, 14, and 28 are dependent on claims 1, 10, and 23, respectively; therefore the rejection of claims 1, 10, and 23 are incorporated as if fully recited herein.

Liang teaches wherein the service provider aggregates notifications provided by different consumer systems to determine whether the application should be authorized to request services of the service provider (paragraph 46; "the correlative rules engine accordingly collects the abnormality events from a plurality of client devices and determines the statistical results").

**Referring to claim 6, 15, and 29:**

Claims 6, 15, and 29 are dependent on claims 1, 10, and 23, respectively; therefore the rejection of claims 1, 10, and 23 are incorporated as if fully recited herein.

Liang teaches the service provider aggregates notifications provided by the consumer system to determine whether the

consumer system should not be authorized to request services of the service provider (paragraphs 38; "the data processor reports abnormalities if abnormal events are detected in a client device").

**Referring to claims 11 and 26:**

Claims 11 and 26 are dependent on claims 10 and 23, respectively; therefore the rejection of claims 10 and 23 are incorporated as if fully recited herein.

Liang teaches wherein the indication of misbehavior is exceeding a number of requests for services of the service provider (paragraphs 30-31; "issue high-risk alerts if the data reach or exceed certain thresholds" and "including activities such as connecting or downloading from the web" where use of network resources is interpreted as a request for services).

**Referring to claims 13 and 27:**

Claims 13 and 27 are dependent on claims 10 and 23, respectively; therefore the rejection of claims 10 and 23 are incorporated as if fully recited herein.

Liang teaches before installing the application determining whether the application is authorized to request services of the service provider (paragraphs 28-30; where it is implied that the anti-virus system will prevent the installation of applications which have been detected to include a virus and the service

being provided is the use of the processor or network resources by the application).

**Referring to claim 17:**

Liang teaches

when service consumers determine that the application is misbehaving, receiving notifications of the misbehavior from the service consumers, wherein the application misbehaves when the application requests certain services of the service provider (paragraph 35; "storing the abnormality rules in a data processor for each of the plurality of clients in the network system");

determining by the processor whether a condition of misbehavior is satisfied based on the received notifications from different consumers indicating that the application is misbehaving when executed by the different consumers (paragraph 46; "the correlative rules engine accordingly collects the abnormality events from a plurality of client devices and determines the statistical results"); and

when a service request is received to provide services to the application and it is determined that the condition of misbehavior is satisfied, refusing to provide the requested service (paragraphs 28-30 and 56; where it is implied that when

the anti-virus system does detect a virus, the request for services will be refused).

**Referring to claim 18:**

Claim 18 is dependent from claim 17; therefore, the rejection of claim 17 is hereby incorporated as if fully recited herein.

Liang teaches wherein the condition of misbehavior is when multiple service consumers provide notifications that the application has attempted to exceed an established limit of requests for services from the service provider (paragraph 46; "the correlative rules engine accordingly collects the abnormality events from a plurality of client devices and determines the statistical results").

**Referring to claim 19:**

Claim 19 is dependent from claim 17; therefore, the rejection of claim 17 is hereby incorporated as if fully recited herein.

Liang teaches receiving from another service provider a notification that the application is misbehaving wherein the condition of misbehavior is satisfied based on the notification received from another service provider (paragraph 46; "the correlative rules engine accordingly collects the abnormality events from a plurality of client devices and determines the

statistical results" implies that notification of misbehavior may come from another of the "plurality" of service providers).

**Referring to claim 20:**

Claim 20 is dependent from claim 17; therefore, the rejection of claim 17 is hereby incorporated as if fully recited herein.

Liang teaches notifying service consumers that the application is not authorized to request services of the service provider (paragraph 45; "the new alert level will be transferred to the client devices").

**Referring to claim 21:**

Claim 21 is dependent from claim 20; therefore, the rejection of claim 20 is hereby incorporated as if fully recited herein.

Liang teaches wherein a service consumer requests the service provider to indicate whether the application is authorized (paragraph 54; "the rules provider can periodically update").

**Referring to claim 22:**

Claim 22 is dependent from claim 17; therefore, the rejection of claim 17 is hereby incorporated as if fully recited herein.

Liang teaches wherein the condition of misbehavior is based on an aggregation of the service consumer notifications (paragraph 46; "the correlative rules engine accordingly collects the abnormality events from a plurality of client devices and determines the statistical results").

**Referring to claim 24:**

Claim 24 is dependent on claim 23; therefore, the rejection of claim 23 is incorporated as if recited herein.

Liang teaches prohibiting execution of the application when the application behaves in accordance with the indication of misbehavior (paragraphs 25-30 and 54-56; "a segment in the network system including the abnormal device nodes can be partially isolated").

6. **Claims 2, 12, and 25 are rejected** under 35 U.S.C. 103(a) as being unpatentable over Liang et al. (US 20040205419) as applied to claims 1, 10, and 24, above, in view of Davis et al. (US 20030135509).

Liang does not disclose wherein the prohibiting includes uninstalling the application. However, Davis discloses wherein the prohibiting includes uninstalling the application (paragraph 64). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the teaching of Liang by uninstalling the application as taught by Davis

because this would provide a way to completely remove an application that was misbehaving.

7. **Claim 9 is rejected** under 35 U.S.C. 103(a) as being unpatentable over Liang et al. (US 20040205419) as applied to claim 1, above, in view of Choate (US 20010054026).

**Referring to claim 9:**

Claim 9 is dependent on claim 1; therefore the rejection of claim 1 is incorporated as if fully recited herein.

Liang does not teach wherein multiple service providers can provide equivalent services and the application can requests services one of those service providers as designated by the consumer system. However, Choate teaches wherein multiple service providers can provide equivalent services and the application can requests services one of those service providers as designated by the consumer system (paragraph 26). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the teaching of Liang as taught by Choate because this would provide the ability to continue to provide services to customers while the system is fixed.

8. **Claims 16 and 30 are rejected** under 35 U.S.C. 103(a) as being unpatentable over Liang et al. (US 20040205419) as applied to claims 10 and 23, above, in view of Choate (US 20010054026).

Liang does not teach wherein the limit is established by a user of a consumer system. However, Choate teaches wherein the limit is established by a user of a consumer system (paragraph 31). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the teaching of Liang by allowing the user to establish a limit as taught by Choate because the user is the one who is actually using the services and is in the best position to determine what is abnormal, which would provide a more accurate assessment of whether the system is misbehaving.

***Conclusion***

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

***Contact***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARRIE A. STRODER whose telephone number is (571)270-7119. The examiner can normally be reached on Monday - Thursday 8:00 a.m. - 5:00 p.m. ET.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jan Mooneyham can be reached on (571)272-6805. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CARRIE A. STRODER/
Examiner, Art Unit 3689

/Tan Dean D. Nguyen/
Primary Examiner, Art Unit 3689
3/27/09